CLAIMS

1. A multiplication module, including a first input unit and a second input unit, for multiplying m bits of data in a Galois field $GF(2^m)(m>=1)$, comprising:

first and second power arithmetic means for receiving the first m bits of data from said first input unit;

first multiplication means for receiving said first m bits of data and the output of said first power arithmetic means;

second multiplication means for receiving second m bits of data from said second input unit and the output of said second power arithmetic means;

selection means for receiving an output signal from said second multiplication means and said second m bits of data; and

control means for outputting a control signal to said first power arithmetic means, said second arithmetic means and said selection means,

wherein said first power arithmetic means receives a first control signal, said second power arithmetic means receives a second control signal, and said selection means receives a third control signal, for controlling the output of said selection means, while said first multiplication means outputs a first output signal, and said selection means outputs a second output signal.

2. A multiplicative inverse arithmetic circuit comprising:

the multiplication module according to claim 1;

first register means for setting a first initial value and for receiving a first output signal from said multiplication module; and

second register means for setting a second initial value and for receiving a second output signal from said multiplication module,

wherein the output terminal of said first register means is connected to said first input unit of said multiplication module, and the output terminal of said second register means is connected to said second input unit of said multiplication module, and

wherein said second register means provides the multiplicative inverse of said first initial value in accordance with said first, second and third control signals.

3. The multiplicative inverse arithmetic circuit according to claim 2, wherein said first and said second register means respectively receive said first initial value and said second initial value; wherein, when the cycle count reaches a predetermined number k (k is a natural number), said control means receives a first control signal for permitting said first power arithmetic means to calculate s powers using $r=2^{k-1}$ and $s=2^r$, and a second control signal for permitting said second power arithmetic means to calculate s powers using $r=\{(m-1) \bmod (2^{k-1})\}+1$ and $s=2^r$; and wherein said selection means of said multiplication means receives a third control signal according to which, when bit k-1 in the binary expression for (m-1) is 1, the output of said second power multiplication means is transmitted to the input terminal of said second register means, and according to which, when bit k-1 in the binary expression for (m-1) is not 1, the output of said second register means is transmitted to the input terminal of said second register means.

4. A multiplicative inverse arithmetic circuit comprising:

two multiplication modules according to claim 1;

first register means for setting a first initial value; and

second register means for setting a second initial value,

wherein a first output of one of said multiplication modules is connected to said first input unit of the other multiplication module, and a second output of one of said multiplication modules is connected to said second input unit of the other multiplication module, and

wherein, for a circuit formed by connecting said multiplication modules, the output terminal of said first register means is connected to said first input units of said multiplication modules, the output terminal of said second register means is connected to said second input units of said multiplication modules, the input terminal of said first register means is connected to said first output units of said multiplication modules, and the input terminal of said second register means is connected to said second output units of said multiplication modules.

5. A multiplicative inverse arithmetic circuit comprising:

at least three multiplication modules according to claim 1;

first register means for setting a first initial value; and

second register means for setting a second initial value,

wherein a first output of one of said multiplication modules is connected to said first input unit of the other multiplication module, and a second output of one of said multiplication modules is connected to said second input unit of the other multiplication module, and

wherein, for a circuit formed by connecting said multiplication modules, the output terminal of said first register means is connected to said first input units of said multiplication modules, the output terminal of said second register means is connected to said second input units of said multiplication modules, the input terminal of said first register

means is connected to said first output units of said multiplication modules, and the input terminal of said second register means is connected to said second output units of said multiplication modules.

6. The multiplicative inverse arithmetic circuit according to claim 4, wherein the number n (n is a natural number) of said multiplication modules is set equal to or smaller than $[\log_2(m-1)+1]$.

7. The multiplicative inverse arithmetic circuit according to claim 4, wherein, when the cycle count reaches a predetermined number q (q is a natural number), said control means transmits to the i-th ($n \geq i \geq 1$) multiplication module a first control signal, which permits said first power arithmetic means to calculate s powers using $r=2^{p-1}$ and $s=2^r$, and a second control signal, which permits said second power arithmetic means to calculate s powers using $r=\{(m-1) \bmod (2^{p-1})\}+1$ and $s=2^r$, while $p=\{n(q-1)+i\}$; wherein said selection means of said i-th multiplication module receives a third control signal according to which, when bit p-1 in the binary expression (m-1) is 1, the output of said second power multiplication means is transmitted to the second output terminal of said i-th multiplication module, and when bit p-1 in the binary expression (m-1) is not 1, m bit data for said second input unit of said i-th multiplication module is transmitted to the second output terminal of said i-th multiplication module.

8. A multiplicative inverse arithmetic circuit comprising:

$[\log_2(m-1)+1]$ multiplication modules according to claim 1; and

control means, for providing a first control signal group, a second control signal group and a third control signal group for respectively controlling said multiplication modules,

wherein the first output terminal of each of said multiplication modules is connected to the first input terminal of a succeeding multiplication module, and the second output terminal of each of said multiplication modules is connected to the second input terminal of a succeeding multiplication module, and

wherein said control means provides for first power arithmetic means a first control signal for permitting a k-th (k is a natural number) multiplication module to calculate s powers using $r=2^{k-1}$ and $s=2^r$, provides for second power arithmetic means a second control signal for permitting said k-th multiplication module to calculate s powers using $r=\{(m-1) \bmod (2^{k-1})\}+1$ and $s=2^r$, provides the output of said second multiplication means as the output of selection means, when bit k-1 in binary expression of m-1 is 1, and provides, as the output of said selection means, m bits of data received from said second input unit when said bit k-1 in the binary expression m-1 is not 1.

9. The multiplicative inverse arithmetic circuit according to claim 8, further comprising:

a pair of register means connected to said multiplication means.

10. A method for controlling a multiplication module, including a first input unit and a second input unit, for multiplying m bits of data in a Galois field $GF(2^m)$ $(m \geq 1)$, comprising the steps of:

inputting the first m bits of data from said first input unit to first and second power arithmetic means;

inputting, to first multiplication means, said first m bits of data and the output of said first power arithmetic means;

inputting, to second multiplication means, second m bits of data from said second input unit and the output of said second power arithmetic means;

inputting, to selection means, an output signal from said second multiplication means and said second m bits of data; and

outputting a control signal to said first multiplication means, said second multiplication means and said selection means,

wherein said first power arithmetic means receives a first control signal, said second power arithmetic means receives a second control signal, and said selection means receives a third control signal, for controlling the output of said selection means, while said first multiplication means outputs a first output signal, and said selection means outputs a second output signal.

11. A method for controlling a multiplicative inverse arithmetic circuit comprising the steps of:

providing a multiplication module according to claim 1;

providing a first register means for setting a first initial value and for receiving a first output signal from said multiplication module; and

providing second register means for setting a second initial value and for receiving a second output signal from said multiplication module,

wherein the output terminal of said first register means is connected to said first input unit of said multiplication module, and the output terminal of said second register means is connected to said second input unit of said multiplication module, and

wherein said second register means provides the multiplicative inverse of said first initial value in accordance with said first, second and third control signals.

12. The method for controlling a multiplicative inverse arithmetic circuit according to claim 11, further comprising the steps of:

receiving said first initial value and said second initial value;

when the cycle count reaches a predetermined number k (k is a natural number), receiving a first control signal for permitting said first power arithmetic means to calculate s powers using $r=2^{k-1}$ and $s=2^r$, and a second control signal for permitting said second power arithmetic means to calculate s powers using $r=\{(m-1) \bmod (2^{k-1})\}+1$ and $s=2^r$;

inputting, to said selection means of said multiplication module, a third control signal according to which, when bit k-1 in the binary expression for (m-1) is 1, the output of said second power multiplication means is transmitted to the input terminal of said second register means, and according to which, when bit k-1 in the binary expression for (m-1) is not 1, the output of said second register means is transmitted to the input terminal of said second register means.

13. A method for controlling a multiplicative inverse arithmetic circuit that includes two multiplication modules according to claim 1, first register means for setting a first initial value, and second register means for setting a second initial value, wherein a first output of one of said multiplication modules is connected to said first input unit of the other multiplication module, and a second output of one of said multiplication modules is connected to said second input unit of the other multiplication module, said method comprising the steps of:

for a circuit formed by connecting said multiplication modules, connecting the output terminal of said first register

means to said first input units of said multiplication modules; and

connecting the output terminal of said second register means to said second input units of said multiplication modules.

14. A method for controlling a multiplicative inverse arithmetic circuit that includes at least three multiplication modules according to claim 1, first register means for setting a first initial value, and second register means for setting a second initial value, wherein a first output of one of said multiplication modules is connected to said first input unit of the other multiplication module, and wherein a second output of one of said multiplication modules is connected to said second input unit of the other multiplication module, said method comprising the steps of:

for a circuit formed by connecting said multiplication modules, connecting the output terminal of said first register means to said first input units of said multiplication modules; and

connecting the output terminal of said second register means to said second input units of said multiplication modules.

15. The method for controlling a multiplicative inverse arithmetic circuit according to claim 13, wherein the number n (n is a natural number) of said multiplication modules is set equal to or smaller than $[\log_2(m-1)+1]$.

16. The method for controlling a multiplicative inverse arithmetic circuit according to claim 13, further comprising the steps of:

when the cycle count reaches a predetermined number q (q is a natural number), transmitting, to the i-th ($n \geq i \geq 1$) multiplication

module, a first control signal, which permits said first power arithmetic means to calculate s powers using $r=2^{p-1}$ and $s=2^r$, and a second control signal, which permits said second power arithmetic means to calculate s powers using $r=\{(m-1) \bmod (2^{p-1})\}+1$ and $s=2^r$, while $p=\{n(q-1)+i\}$; and

transmitting, to said selection means of said i-th multiplication module, a third control signal according to which, when bit p-1 in the binary expression (m-1) is 1, the output of said second multiplication means is transmitted to the second output terminal of said i-th multiplication module, and when bit p-1 in the binary expression (m-1) is not 1, m bit data for said second input unit of said i-th multiplication module is transmitted to the second output terminal of said i-th multiplication module.

17. A method for controlling a multiplicative inverse arithmetic circuit comprising the steps of:

providing $[\log_2(m-1)+1]$ multiplication modules according to claim 1; and

providing a first control signal group, a second control signal group and a third control signal group for respectively controlling said multiplication modules, with the first output terminal of each of said multiplication modules being connected to the first input terminal of a succeeding multiplication module, and the second output terminal of each of said multiplication modules being connected to the second input terminal of a succeeding multiplication module,

providing, for first power arithmetic means, a first control signal for permitting a k-th (k is a natural number) multiplication module to calculate s powers using $r=2^{k-1}$ and $s=2^r$;

providing, for second power arithmetic means, a second control signal for permitting said k-th multiplication module to calculate s powers using $r=\{(m-1) \bmod(2^{k-1})\}+1$ and $s=2^r$;

providing the output of said second multiplication means as the output of selection means, when bit k-1 in binary expression of m-1 is 1; and

providing, as the output of said selection means, m bits of data received from said second input unit when said bit k-1 in the binary expression m-1 is not 1.

18. The method for controlling a multiplicative inverse arithmetic circuit according to claim 12, further comprising the step of:

transmitting the output from said multiplication module to a pair of register means.

19. An apparatus employing a multiplication module, including a first input unit and a second input unit, for multiplying m bits of data in a Galois field $GF(2^m)(m \geq 1)$, said multiplication module comprising:

first and second power arithmetic means for receiving the first m bits of data from said first input unit;

first multiplication means for receiving said first m bits of data and the output of said first power arithmetic means;

second multiplication means for receiving second m bits of data from said second input unit and the output of said second power arithmetic means;

selection means for receiving an output signal from said second multiplication means and said second m bits of data; and

control circuit for outputting a control signal to said first power arithmetic means, said second power arithmetic means and said selection means,

wherein said first power arithmetic means receives a first control signal, said second power arithmetic means receives a second control signal, and said selection means receives a third control signal, for controlling the output of said selection means, while said first multiplication means outputs a first output signal, and said selection means outputs a second output signal.

20. An apparatus including a multiplicative inverse arithmetic circuit that comprises:

the multiplication module according to claim 1;

first register means for setting a first initial value and for receiving a first output signal from said multiplication module; and

second register means for setting a second initial value and for receiving a second output signal from said multiplication module,

wherein the output terminal of said first register means is connected to said first input unit of said multiplication module, and the output terminal of said second register means is connected to said second input unit of said multiplication module, and

wherein said second register means provides the multiplicative inverse of said first initial value in accordance with said first, second and third control signals.

21. The apparatus according to claim 20, wherein said first and said second register means respectively receive said first initial value and said second initial value; wherein, when the cycle count reaches a predetermined number k (k is a natural number), said control means receives a first control signal for permitting said first power arithmetic means to calculate s powers using $r=2^{k-1}$ and $s=2^{r}$, and a second control signal for permitting said second power

arithmetic means to calculate s powers using $r=\{(m-1)\bmod(2^{k-1})\}+1$ and $s=2^r$; and wherein said selection means of said multiplication means receives a third control signal according to which, when bit k-1 in the binary expression for (m-1) is 1, the output of said second multiplication means is transmitted to the input terminal of said second register means, and according to which, when bit k-1 in the binary expression for (m-1) is not 1, the output of said second register means is transmitted to the input terminal of said second register means.

22. An apparatus including a multiplicative inverse arithmetic circuit that comprises:

two multiplication modules according to claim 1;

first register means for setting a first initial value; and

second register means for setting a second initial value,

wherein a first output of one of said multiplication modules is connected to said first input unit of the other multiplication module, and a second output of one of said multiplication modules is connected to said second input unit of the other multiplication module, and

wherein, for a circuit formed by connecting said multiplication modules, the output terminal of said first register means is connected to said first input units of said multiplication means, the output terminal of said second register means is connected to said second input units of said multiplication modules, the input terminal of said first register means is connected to said first output units of said multiplication means, and the input terminal of said second register means is connected to said second output units of said multiplication modules.

23. An apparatus including a multiplicative inverse arithmetic circuit that comprises:

at least three multiplication modules according to claim 1;

first register means for setting a first initial value; and

second register means for setting a second initial value,

wherein a first output of one of said multiplication modules is connected to said first input unit of the other multiplication module, and a second output of one of said multiplication modules is connected to said second input unit of the other multiplication module, and

wherein, for a circuit formed by connecting said multiplication modules, the output terminal of said first register means is connected to said first input units of said multiplication modules, the output terminal of said second register means is connected to said second input units of said multiplication modules, the input terminal of said first register means is connected to said first output units of said multiplication means, and the input terminal of said second register means is connected to said second output units of said multiplication modules.

24. The apparatus according to claim 22, wherein the number n (n is a natural number) of said multiplication modules is set equal to or smaller than $[\log_2(m-1)+1]$.

25. The apparatus according to claim 22, wherein, when the cycle count reaches a predetermined number q (q is a natural number), said control means transmits to the i-th ($n \geq i \geq 1$) multiplication module a first control signal, which permits said first power arithmetic means to calculate s powers using $r=2^{p-1}$ and $s=2^r$, and a second control signal, which permits said second power arithmetic means to calculate s powers using $r=\{(m-1) \bmod (2^{p-1})\}+1$ and $s=2^r$,

while $p=\{n(q-1)+i\}$; and wherein said selection means of said i-th multiplication module receives a third control signal according to which, when bit p-1 in the binary expression (m-1) is 1, the output of said second multiplication means is transmitted to the second output terminal of said i-th multiplication module, and when bit p-1 in the binary expression (m-1) is not 1, m bit data for said second input unit of said i-th multiplication module is transmitted to the second output terminal of said i-th multiplication module.

26. An apparatus including a multiplicative inverse arithmetic circuit that comprises:

$[\log_2(m-1)+1]$ multiplication modules according to claim 1; and

control means, for providing a first control signal group, a second control signal group and a third control signal group for respectively controlling said multiplication modules,

wherein the first output terminal of each of said multiplication modules is connected to the first input terminal of a succeeding multiplication module, and the second output terminal of each of said multiplication modules is connected to the second input terminal of a succeeding multiplication module, and

wherein said control means provides for first power arithmetic means a first control signal for permitting a k-th (k is a natural number) multiplication module to calculate s powers using $r=2^{k-1}$ and $s=2^r$, provides for second power arithmetic means a second control signal for permitting said k-th multiplication module to calculate s powers using $r=\{(m-1)\bmod(2^{k-1})\}+1$ and $s=2^r$, provides the output of said second multiplication means as the output of selection means, when bit k-1 in binary expression of m-1 is 1, and provides, as the output of said selection means, m

bits of data received from said second input unit when said bit k-1 in the binary expression m-1 is not 1.

27. The apparatus according to claim 22, wherein said multiplicative inverse arithmetic circuit further comprises:

a pair of register means connected to said multiplication means.

28. A method, for controlling a multiplicative inverse arithmetic circuit, comprising the steps of:

transmitting, to multiplication means, m bits of data from a first input unit and the output of power arithmetic means in order to multiply said m bits of data in a Galois field $GF(2^m)$ $(m \geq 1)$;

transmitting, to multiplication means, m bits of data from a second input unit and the output of said power arithmetic means;

transmitting a first control signal, which permits said first power arithmetic means to calculate s powers using $r=2^{p-1}$ and $s=2^r$, and a second control signal, which permits said second power arithmetic means to calculate s powers using $r=\{(m-1) \bmod (2^{p-1})\}+1$ and $s=2^r$, while $p=\{n(q-1)+i\}$; and

providing the output of said second multiplication means as the output of selection means, when bit k-1 in binary expression of m-1 is 1, and providing, as the output of said selection means, m bits of data received from said second input unit when said bit k-1 in the binary expression m-1 is not 1.

29. A computer-readable recording medium on which source code is recorded that permits a computer to execute a multiplication method comprising the steps of:

transmitting, to multiplication means, m bits of data from a first input unit and the output of power arithmetic means in order to multiply said m bits of data in a Galois field $GF(2^m)$ $(m \geq 1)$;

transmitting, to multiplication means, m bits of data from a second input unit and the output of said power arithmetic means;

transmitting a first control signal, which permits said first power arithmetic means to calculate s powers using $r=2^{p-1}$ and $s=2^r$, and a second control signal, which permits said second power arithmetic means to calculate s powers using $r=\{(m-1)\bmod(2^{p-1})\}+1$ and $s=2^r$, while $p=\{n(q-1)+i\}$; and

providing the output of said second multiplication means as the output of selection means, when bit k-1 in binary expression of m-1 is 1, and providing, as the output of said selection means, m bits of data received from said second input unit when said bit k-1 in the binary expression m-1 is not 1.

30. A computer-readable transfer medium on which source code is recorded that permits a computer to execute a multiplication method comprising the steps of:

transmitting, to multiplication means, m bits of data from a first input unit and the output of power arithmetic means in order to multiply said m bits of data in a Galois field $GF(2^m)(m \geq 1)$;

transmitting, to multiplication means, m bits of data from a second input unit and the output of said power arithmetic means;

transmitting a first control signal, which permits said first power arithmetic means to calculate s powers using $r=2^{p-1}$ and $s=2^r$, and a second control signal, which permits said second power arithmetic means to calculate s powers using $r=\{(m-1)\bmod(2^{p-1})\}+1$ and $s=2^r$, while $p=\{n(q-1)+i\}$; and

providing the output of said second multiplication means as the output of selection means, when bit k-1 in binary expression of m-1 is 1, and providing, as the output of said selection means, m bits of data received from said second input unit when said bit k-1 in the binary expression m-1 is not 1.

31. A cryptographic apparatus comprising:

multiplication means for receiving m bits of data from a first input unit and the output of power arithmetic means in order to multiply said m bits of data in a Galois field $GF(2^m)$ $(m \geq 1)$;

multiplication means for receiving m bits of data from a second input unit and the output of said power arithmetic means;

means for transmitting, to a first power arithmetic means, a first control signal that permits said first power arithmetic means to calculate s powers using $r=2^{p-1}$ and $s=2^r$, and for transmitting, to a second power arithmetic means, a second control signal that permits said second power arithmetic means to calculate s powers using $r=\{(m-1) \bmod (2^{p-1})\}+1$ and $s=2^r$, while $p=\{n(q-1)+i\}$; and

means for providing the output of said second multiplication means as the output of selection means, when bit k-1 in binary expression of m-1 is 1, and providing, as the output of said selection means, m bits of data received from said second input unit when said bit k-1 in the binary expression m-1 is not 1.

32. An error correction decoder comprising:

multiplication means for receiving m bits of data from a first input unit and the output of power arithmetic means in order to multiply said m bits of data in a Galois field $GF(2^m)$ $(m \geq 1)$;

multiplication means for receiving m bits of data from a second input unit and the output of said power arithmetic means;

means for transmitting, to a first power arithmetic means, a first control signal that permits said first power arithmetic means to calculate s powers using $r=2^{p-1}$ and $s=2^r$, and for transmitting, to a second power arithmetic means, a second control signal that permits said second power arithmetic means to calculate s powers using $r=\{(m-1) \bmod (2^{p-1})\}+1$ and $s=2^r$, while $p=\{n(q-1)+i\}$; and

means for providing the output of said second multiplication means as the output of selection means, when bit k-1 in binary expression of m-1 is 1, and providing, as the output of said selection means, m bits of data received from said second input unit when said bit k-1 in the binary expression m-1 is not 1.

33. An apparatus comprising:

multiplication means for receiving m bits of data from a first input unit and the output of power arithmetic means in order to multiply said m bits of data in a Galois field $GF(2^m)(m \geq 1)$;

multiplication means for receiving m bits of data from a second input unit and the output of said power arithmetic means;

means for transmitting, to a first power arithmetic means, a first control signal that permits said first power arithmetic means to calculate s powers using $r=2^{p-1}$ and $s=2^r$, and for transmitting, to a second power arithmetic means, a second control signal that permits said second power arithmetic means to calculate s powers using $r=\{(m-1)\bmod(2^{p-1})\}+1$ and $s=2^r$, while $p=\{n(q-1)+i\}$; and

means for providing the output of said second multiplication means as the output of selection means, when bit k-1 in binary expression of m-1 is 1, and providing, as the output of said selection means, m bits of data received from said second input unit when said bit k-1 in the binary expression m-1 is not 1.